Remarks

Reconsideration of this Application is respectfully requested.

Upon entry of the foregoing amendment, claims 1-6, 10-12, 16-22, and 40-51 are pending in the application, with claims 1, 16, and 40 being the independent claims. Claims 7-9, 13-15, and 23-39 were previously cancelled without prejudice to or disclaimer of the subject matter recited therein. Claims 1, 2, 4, 16, 40-43, and 51 are sought to be amended. Support for the amendments is found in the instant specification, at least at, for example, paragraphs [0008], [0013], [0017], [0028] - [0039], [0051] - [0061], and [0065] and FIGs. 2 - 6, 8 and 9 and originally filed claims 1 and 40. Applicant reserves the right to prosecute similar or broader claims, with respect to the cancelled and amended claims, in the future.

These changes are believed to introduce no new matter, and their entry is respectfully requested.

Based on the above amendment and the following remarks, Applicant respectfully requests that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

Statement of Substance of Examiner Interview

Applicant submits the following Statement of Substance of Interviews conducted between the Examiner and Applicant's representative, Randall K. Baldwin, on August 5, 2010. Applicant's representative gratefully acknowledges the courtesies extended by the Examiner in granting a telephone interview on August 5, 2010. In the interview, the Examiner clarified the objections to claims 2, 19, and 41-43 and the rejection of claims

40-43 and 51 under 35 U.S.C. § 101. During the interview, the Examiner and Applicant's representative discussed proposed claim amendments and the Examiner agreed that the proposed amendments would overcome the rejection under 35 U.S.C. § 101 of claims 40-43 and 51 and the objections to claims 2, 19, and 41-43 due to informalities. The Examiner also clarified comments regarding his interpretation of the teachings of the applied references. In particular, the Examiner clarified his comments regarding independent claims 1, 16, and 40 and the teachings of Schreiber and Garcia. Applicant's representative discussed distinctions between claims 1, 16, and 40 and the applied references. No specific agreement was reached.

The substance of the discussion and arguments in the telephone interview is included in the present remarks.

Claim Objections

On page 2 of the Office Action, claims 2, 19, and 41-43 were objected to due to informalities. As discussed during the aforementioned telephonic interview, Applicant submits herewith amended claims 2, 19 and 41-43 pursuant to the Examiner's suggestions indicated on page 2 of the Office Action that address the Examiner's concerns. Accordingly, Applicant respectfully requests reconsideration and withdrawal of the objection to claims 2, 19 and 41-43.

Rejection under 35 U.S.C. § 101

At page 2 of the Office Action the Examiner rejected claims 40-43 and 51 under 35 U.S.C. § 101 as being allegedly directed to non-statutory subject matter because the

"computer readable medium" recited in these claims could be interpreted to include non-statutory subject matter. Applicant respectfully traverses this rejection.

During the aforementioned interview and on page 3 of the Office Action, the Examiner suggested amending the claims such that they recite a "non-transitory" computer readable medium. Although the Applicant disagrees with the rejection, merely in order to expedite prosecution, and without acquiescing to the propriety of the rejection, claim 40 is amended herein to include the suggested language.

Amended claim 40 recites, *inter alia*, "[a] non-transitory computer readable medium having instructions stored thereon for restricting the use of a clipboard application."

Claims 41-43 and 51 as amended are directed to non-transitory computer readable media. Support for these amendments is found in the specification, at least at, for example, paragraphs [0013] and [0065] and FIG. 9 and originally filed claim 40.

Applicant understands the term "non-transitory" to merely exclude "computer readable medium" from reading on non-tangible media such as signals and waveforms, and that no further restriction of the claim scope is introduced through this amendment.

Applicant notes that a "non-transitory computer-readable medium," as recited by claims 40-43 and 51, comprises all computer-readable media, with the sole exception being a transitory, propagating signal. By way of example and not limitation, the specification describes exemplary embodiments wherein "[t]he invention can also be embodied as computer readable code on a computer readable medium . . . [t]he computer readable medium is any data storage device that can store data which can thereafter be read by a computer system" and "[e]xamples of the computer readable medium include

read-only memory, random-access memory, CD-ROMs, magnetic tape, [and] optical data storage devices" (Applicant's specification, paragraph [0065]).

Claims 41-43 and 51 depend from claim 40 and, thus, include the "non-transitory computer-readable medium" language as well. Therefore, claims 40-43 and 51 are directed to statutory subject matter.

Accordingly, at least based on the amendments above, Applicant respectfully requests that the rejection of claims 40-43 and 51 under 35 U.S.C. § 101 be reconsidered and withdrawn.

Rejections under 35 U.S.C. § 103

At page 2 of the Office Action the Examiner rejected claims 1-4, 10-12, 16-20, 40, 42, 45, and 47-51 under 35 U.S.C. § 103(a) as being allegedly unpatentable over U.S. Pub. No. 2001/0000265 to Schreiber *et al.* ("Schreiber") in view of U.S. Pat. No. 7,178,033 to Garcia ("Garcia").

Claims 5, 6, 21, and 22 were rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Schreiber in view of Garcia, and further in view of Adobe Acrobat 5.0 ("Adobe").

Claims 41 and 43 were rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Schreiber in view of Garcia, and further in view of U.S. Pub. No. 2002/0052981 to Yasuda ("Yasuda").

Claims 44 and 46 were rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Schreiber in view of Garcia further, and further in view of U.S. Pat. No. 7,281,272 to Rubin *et al.* ("Rubin"). Applicant respectfully traverses these rejections for the reasons stated below.

As discussed during the aforementioned interview, without acquiescing to the propriety of the rejections, and merely to expedite prosecution, Applicant has amended claims 1, 2, 4, 16, 40-43, and 51.

Applicant submits that the applied references, singly, or in the allegedly obvious combination do not describe each and every element as set forth in independent claims 1, 16, and 40.

Claims 1 and 16 as amended herein recite, using respective language, among other features:

> receiving a copy command associated with the copy selection, the copy command including a password associated with a user;
> authenticating the user based upon the received password; and
> determining whether the source file is a secured file, wherein the secured file includes a header having a file key available to the authenticated user[.]

Further, for example, claim 40 as amended herein recites, *inter alia*:

> instructions to receive a copy command associated with the copy selection, the copy command including a password associated with a user;
> instructions to authenticate the user based upon the received password; and
> instructions to determine whether the source file is a secured file, wherein the secured file includes a header having a file key available to the authenticated user[.]

Applicant respectfully submits that the applied references, in the sections cited by the Examiner, or in other sections, contain no teaching or suggestion of at least the above-noted distinguishing features of amended claims 1, 16, and 40.

Schreiber teaches that "the user views the web page, and . . . attempts to copy the embedded image by executing a command to copy pixel data of the image from a video buffer to a clipboard," "the client computer calls an operating system function . . . to

extract pixel data from the video buffer and copy it to the clipboard," and "the data returned from the operating system function is written to the clipboard and at step 824 the user pastes the data from the clipboard into a window of another software application, or save it into his computer." (Schreiber, paragraphs [0136] - [0138] and FIG. 8). However, nowhere does Schreiber teach or suggest "receiving a copy command associated with the copy selection, the copy command including a password associated with a user; authenticating the user based upon the received password; and determining whether the source file is a secured file, wherein the secured file includes a header having a file key available to the authenticated user," as recited, using respective similar language, in claims 1, 16, and 40. As discussed during the interview, Applicant respectfully submits that Schreiber's "method for preventing unauthorized copying of digital images within a client computer" (Schreiber, paragraph [0135]) does not teach or suggest the above-noted "receiving a copy command," "authenticating the user," and "determining whether the source file is a secured file" recited in claims 1, 16, and 40.

With reference to previously pending claims 1, 16, and 40, the Examiner acknowledges that Schreiber "fails to explicitly disclose determining whether the source file is a secured file, wherein the secured file includes a header requiring a file key obtained by an authenticated user to access the protected file." (Office Action, page 3). Rather, the Examiner relies on the Garcia to cure the acknowledged deficiencies of Schreiber.

With regards to Garcia, the Examiner states, which Applicant does not concede, that "Garcia teaches determining whether a file is a secure file, wherein the secure file includes a header requiring a file key obtained by an authenticated user to access the protected file" and that "[a]t the time of the invention it would have been obvious to a

person of ordinary skill in the art to determine whether the content can be used an to require a user to be authenticated to obtain a key to gain access." (Office Action, pages 3-4).

The deficiencies of Schreiber are not cured by Garcia. Garcia is not used by the Examiner to teach or suggest at least the above noted distinguishing features of claims 1, 16, and 40. With reference to previously pending claims 1, 16, and 40, the Examiner asserts that lines 18-31 of column 12 of Garcia teach " determining whether a file is a secure file, wherein the secure file includes a header requiring a file key obtained by an authenticated user to access the protected file " (Office Action, pages 4-5). Lines 18-31 of column 12 of Garcia read:

> "The block 342 of the header structure 350 includes at least three segments 344, 346 and 348. The segment 344 includes an encrypted file key that must be retrieved in clear to decrypt the encrypted data portion. The segment 346 includes security level information to indicate what security level the secured file is at, for example, "top secret", "secret", "confidential" or "unclassified" or "none". The segment 348 includes information about the size of the encryption block for the encrypted data portion in the secured file. According to one embodiment, this is a multiple of the algorithm encryption block size. The encrypted data portion is created by an encryption with a symmetric key that is called the document/file-encryption-key or file key herein. "

While Garcia discusses a "header structure" including "an encrypted file key," "security level information," and " information about the size of the encryption block," Applicant respectfully submits that the above-quoted portion of Garcia fails to teach or suggest at least "receiving a copy command associated with the copy selection, the copy command including a password associated with a user; authenticating the user based upon the received password; and determining whether the source file is a secured file, wherein the secured file includes a header having a file key available to the authenticated user," as recited, using respective similar language, in claims 1, 16, and 40.

Thus, the allegedly obvious combination of Schreiber and Garcia does not teach or suggest each and every limitation of claims 1, 16, and 40. For at least these reasons, the cited art does not support the § 103 rejection of independent claims 1, 16, and 40. Reconsideration and allowance of these claims is respectfully requested.

Claims 2-6, 10-12, and 44-49 depend upon claim 1, and the comments above directed to claim 1 apply equally to claims 2-6, 10-12, and 44-49, in addition to the features recited in these dependent claims. See *In Re Fine*, 837 F.2d 1071 (Fed. Cir. 1988) and M.P.E.P. § 2143.03. Accordingly, Applicant respectfully requests that the Examiner reconsider and remove the rejections of claims 2-6, 10-12, and 44-49 under 35 U.S.C. § 103(a) and pass these claims to allowance.

At least based on their respective dependencies to claim 16, claims 17-22 and 50 should be found allowable over the applied references, as well as for their additional distinguishing features.

Claims 41-43 and 51 depend from independent claim 40, and the comments above directed to claim 40 apply equally to claims 41-43 and 51, in addition to the features recited in the claims 41-43 and 51. Accordingly, Applicant respectfully requests that the Examiner reconsider and remove the rejections of claims 41-43 and 51 under 35 U.S.C. § 103(a) and pass these claims to allowance.

At page 5 of the Office Action the Examiner rejected claims 5, 6, 21, and 22 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Schreiber in view of Garcia, and further in view of Adobe.

With reference to claims 5, 6, 21, and 22, the Examiner acknowledges that Schreiber as modified by Garcia fails to disclose "said determining operates to determine that the source file is a secured file based on security information provided by the source

application." (Office Action, page 5). The Examiner asserts, which Applicant does not acquiesce to, that Adobe "teaches such a determination" (Office Action, page 5). Even assuming for the sake of argument that the Examiner's interpretation of the teachings of Adobe is correct, Adobe fails to teach or suggest "receiving a copy command associated with the copy selection, the copy command including a password associated with a user; authenticating the user based upon the received password; and determining whether the source file is a secured file, wherein the secured file includes a header having a file key available to the authenticated user," as recited, using respective similar language, in claims 1, 16, and 40. While Adobe describes that "[u]sers can set passwords to prevent others from viewing, editing or printing certain documents . . . during the editing process" and that Adobe Acrobat PDF files can be password protected (Adobe, pages 28 and 29), Applicant submits that the acknowledged deficiencies of Schreiber and Garcia are not cured by Adobe with respect to claims 5, 6, 21, and 22. Thus, claims 5, 6, 21, and 22 should be found allowable over the applied references for at least this additional reason.

At page 5 of the Office Action the Examiner rejected claims 41 and 43 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Schreiber in view of Garcia, and further in view of Yasuda.

With reference to claims 41 and 43, the Examiner acknowledges that Schreiber as modified by Garcia "fails to explicitly disclose storing scrambled content to the clipboard application in place of the designated content when said determining determines that the source file is a secured file." (Office Action, page 5). Rather, the Examiner relies on the Yasuda to cure the acknowledged deficiencies of Schreiber and Garcia.

Yasuda does not cure the acknowledged and above-noted deficiencies of Schreiber and Garcia. Yasuda describes that "the copy suppress processing part 53 determines whether or not to suppress copying of data" by referring "to the definition file 4 to determine whether or not the clipboard canceller is set to "ON"" (Yasuda, paragraph [0138]). However, Applicant submits that Yasuda's clipboard canceller is not analogous to a file key available to the authenticated user as recited, using respective language, in claims 1, 16, and 40. In contrast to the above-noted distinguishing features of claims 1, 16, and 40, Yasuda describes that "the system manager sets a clipboard canceller to suppress or allow the copy operation by the user . . . sets "ON" to the clipboard canceller in order to suppress copying of data through a clipboard, or the system manager sets "OFF" to the clipboard canceller in order to allow to copy data through the clipboard . . . saves a setting of the clipboard canceller to the definition file" (Yasuda, paragraphs [0130] and [0131]). The clipboard canceller feature discussed in Yasuda is clearly a user-selected (i.e., system manager-selected) binary "ON" "OFF" setting that is saved in a definition file. Yasuda describes that the system manager's selections are made on a ***per-application basis*** in order to suppress or allow application menu items and functions (Yasuda, paragraphs [0053]-[0059] and [0066] and FIGs. 1 and 3). Thus, Yasuda's selections are not made on a per-source file basis. Therefore, Yasuda lacks any teaching or suggestion of determining whether the source file is a secured file, wherein the secured file includes a header having a file key available to the authenticated user, and wherein the secured file cannot be accessed without the file key, as recited, using respective language, in claims 1, 16, and 40.

Further, Yasuda fails to teach or suggest receiving a copy selection associated with ***designated content*** of a source file being displayed by a first source application, as

recited, using respective similar language, in claims 1, 16, and 40. Yasuda generally describes a system wherein a computer operating system (OS) "transfers data at a copy-from to the clipboard" after "the user conducts a paste instruction for pasting the data copied" (Yasuda, paragraphs [0132]-[0142]). Yasuda discloses that "when the data transferred into the clipboard *is cleared* . . . the clipboard canceller in the definition file 4 is set to "ON" . . . the *original data at the copy-from cannot be copied* (can be prohibited or suppressed)," or "when the clipboard canceller in the definition file 4 is set to "OFF", the original data at the copy-from is copied to the copy-to since the data transferred from the copy-from to the clipboard is not cleared (a normal copy operation via the clipboard is conducted)" (Yasuda, paragraph [0142]) (emphasis added). However, Yasuda does not define what is meant by a "copy-from" and nowhere does Yasuda teach or suggest determining whether the source file is a secured file, wherein the secured file includes a header having a file key available to the authenticated user, and wherein the secured file cannot be accessed without the file key, as recited, using respective similar language, in claims 1, 16, and 40.

Yasuda also fails to teach or suggest "determining whether a copy selection associated with designated content of a source file being displayed by a first source application has been made" or "receiving a copy command associated with the copy selection, the copy command including a password associated with a user," as recited, using respective language, in claims 1 and 16. Instead of instructions to receive a copy command associated with the copy selection, the copy command including a password associated with a user, as recited in claim 40, Yasuda discusses performing data transfers by an OS to a clipboard after "the user conducts a copy operation for copying data on the display unit of the user terminal." (Yasuda, paragraph [0134]). Applicant submits that

an OS data transfer from a display of a user terminal is not analogous to " determining

whether a copy selection associated with designated content of a source file being

displayed by a first source application has been made" and "receiving a copy selection

associated with designated content of a source file being displayed by a first source

application," as respectively recited in claims 1 and 16. Similarly, the data transfer

operation discussed in Yasuda is not analogous to instructions to receive a copy selection

associated with designated content of a source file being displayed by a first source

application, as recited in claim 40.

Yasuda discusses a method to "prohibit copying of data through the clipboard"

by suppressing copying of data and replacing "data with *empty data* in the clipboard"

(Yasuda, paragraphs [0132]-[0139] and [0142]) (emphasis added). Yasuda's method

suppresses copying of data through a clipboard by suppressing the display of an

application menu item (Yasuda, paragraphs [0011], [0012], [0045], and [0143] and FIGs.

1-3). However, nowhere does Yasuda teach or suggest the capability of receiving a copy

command associated with the copy selection, the copy command including a password

associated with a user and determining whether the source file is a secured file, wherein

the secured file includes a header having a file key available to the authenticated user,

and wherein the secured file cannot be accessed without the file key, as recited, using

respective similar language, in claims 1, 16, and 40. Instead, Yasuda prohibits copying

of data by clearing content of a clipboard when the notice for copying data is detected

and copying "the content (actually no data) in the clipboard" (Yasuda, paragraphs

[0016], [0017] and [0048]).

Accordingly, Applicant submits that the acknowledged deficiencies of Schreiber

and Garcia are not cured by Yasuda with respect to claims 41 and 43. Thus, claims 41

and 43 should be found allowable over the applied references for at least this additional reason.

On page 6 of the Office Action, claims 44 and 46 were rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Schreiber in view of Garcia, and further in view of Rubin.

Rubin is not stated by the Examiner to teach or suggest, nor does Rubin teach or suggest, at least the above noted distinguishing features of claim 1. Although Rubin discusses "protecting digital images from being copied from a video RAM" (Rubin, col. 3, lines 56-57), nowhere does Rubin teach or suggest at least the above-noted distinguishing features of claim 1. Therefore, as Schreiber, Garcia, and Rubin do not teach at least the above-noted distinguishing features of claim 1, the applied references cannot be used to establish a *prima facie* case of obviousness with regards to claims 44 and 46, which depend from claim 1.

Thus, claims 44 and 46 should be found allowable over the applied references for at least this additional reason.

Conclusion

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding objections and rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Glenn J. Perry
Attorney for Applicant
Registration No. 28,458

Date: 22 Sept 2010

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600
1132918_1.doc

Atty. Dkt. No. 2222.5600000